

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Infrastructure, Office Automation & Telecommunications (IOAT)

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2Summary of PIA Required Questions

Question

Response

- 1 System:

IHS Infrastructure, Office Automation & Telecommunications (IOAT)
- 2 Is this a new PIA?

No
- 3 If this is an existing PIA, please provide a reason for revision:

Initial PIA Migration to ProSight
- 4 Date of this Submission:

Oct 28, 2003
- 5 OPDIV Name:

IHS
- 6 Unique Project Identifier (UPI) Number:

009-17-02-00-01-1010--110-03; (917020001101000000000)
- 7 Privacy Act System of Records (SOR) Number:

09-90-0006 & 09-7-0002
- 8 OMB Information Collection Approval Number:

No
- 9 Other Identifying Number(s):

No
- 10 System Name:

Infrastruction Office Automation and Telecommunications (IOAT)
- 11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:

Robert McKinney
- 12 Provide an overview of the system:

Allows headquarters and area personnel to post job vacancies and scholarships to the internet and communicate with the IHS administrators of these systems via e-mail via the IHS Network using a secure connection. Potential candidates can search job postings by searching on state, area, and job series keywords. Candidates can apply online using a WORD or PDF document template provided on the website.

Categories of individuals covered by the system: Individuals, including both IHS beneficiaries and non beneficiaries, who are applying for or taking part in job applications or Scholarship & Grants The Jobs database is a database of jobs available throughout IHS facilities, tribally operated health programs, and urban Indian health programs. Authority for maintenance of the system: Section 321 of the Public Health Service Act, as amended, (42 U.S.C. 248), ``Hospitals, Medical Examinations and Medical Care." Section 327A of the Public Health Service Act, as amended, (42 U.S.C. 254a-1), ``Hospital-Affiliated Primary Care Centers." Indian Self Determination and Education Assistance Act (25 U.S.C. 450). Snyder Act (25 U.S.C. 13). Indian Health Care Improvement Act (25 U.S.C. 1601 et. seq). Construction of Community Hospitals Act (25 U.S.C. 2005-2005f). Indian Health Service Transfer Act (42 U.S.C. 2001-2004). In the Indian Health Care Improvement Act (hereinafter the Act), Public Law 94-437, the Congress and the President of the United States established a national goal to provide the quantity and quality of health services which maximum par twill permit the health status of Indians to be raised to the highest possible level and to encourage the participation of Indians in the planning and management of those services. To accomplish this goal, the Indian Health Care Improvement Act (I H C I A) and its subsequent amendments of 1980, 1988, 1992, and 1996 authorize the I H S to conduct three interrelated scholarship programs to train the professional health personnel necessary to staff I H S health programs serving the Indian people. These scholarship programs are the: Health Professions Preparatory Scholarship Program,Section 103(b)(1) Health Professions Pre-graduate Scholarship Program,Section 103(b)(2) Health Professions Scholarship Program,Section 104 Health Professions Extern Program,Section 105.
- 13 Indicate if the system is new or an existing one being modified:

Existing
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?

Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Infrastructure, Office Automation & Telecommunications (IOAT)

15	Is the system subject to the Privacy Act?	Yes
16	If the system shares or discloses IIF please specify with whom and for what purpose(s):	<p>State/Local Health Agencies.</p> <p>A. Records may be disclosed to individuals within the Indian Health Service in the areas of personnel and finance. B. Records may be disclosed to authorized organizations, such as the United States Office of Technology Assessment, or individuals for conduct of analytical and evaluation studies sponsored by the IHS. C. Records may be disclosed to a congressional office in response to an inquiry from that office made at the request of the subject individual. D. A record may be disclosed for a research purpose, when the Department: 1) Has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained; 2) Has determined that the research purpose (1) cannot be reasonably accomplished unless the record is provided in individually identifiable form, and (2) warrants the risk to the privacy of the individual that additional exposure of the record might bring; 3) Has required the recipient to; a. establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, and b. remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining such information, and c. make no further use or disclosure of the record except; i. in emergency circumstances affecting the health or safety of any individual, ii. for use in another research project, under these same conditions, and with written authorization of the Department, iii. for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit, or iv. when required by law; d. Has secured a written statement attesting to the recipient's understanding of, and willingness to abide by these provisions. E. The Department may disclose information from this system of records to the Department of Justice, to a court or other tribunal, or to another party before such tribunal, when:a. HHS, or any component thereof; or b. Any HHS employee in his or her official capacity; or c. Any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or d. The United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the tribunal, or the other party is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected. F. Records may be disclosed to an IHS contractor, including tribal contractors, for the purpose of computerized data entry or maintenance of records contained in this system. The contractor shall be required to maintain Privacy Act safeguards with respect to the receipt and processing of such records.</p>

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Infrastructure, Office Automation & Telecommunications (IOAT)

- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- A. Records containing general information on the person's residence, status of work, phone numbers and also the amount of monies awarded to the individuals using scholarships. These records are maintained and tracked from the beginning of the scholarship process until the person enters employment within the Indian Health.

A. To provide a description of an applicant's interest in applying for jobs advertised within the Indian Health Service. B. To provide IHS program officials with statistical data upon which the jobs and scholarships can be tracked and accounted for. C. To serve as a means of communication among members of the personnel team who contribute to fillings and tracking jobs within the Indian Health Service. D. To serve as the official documentation of jobs begin applied for and scholarships be paid to individual students. E. To contribute to continuing education of IHS staff to improve their competency to deliver health care services and filling jobs within those health care disciplines. F. To improve the IHS health care provides entering the Indian Health Service.
- 18

Describe the consent process:
- Yes, contains IIF. Mandatory submission of personal information. The data is collected via. web-based applications from scholarship applicants and job candidates. Subjects are notified by various messages displayed on the web page. A privacy statement is posted on the site to notify subjects about how their information is handled.
- 19

Does the system host a website?
- Yes
- 20

Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21

Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22

Are there technical controls present?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Infrastructure, Office Automation & Telecommunications (IOAT)

- 23 Describe the IIF security controls:
- Policies and procedures are in place to ensure access, to include physical access, to data and equipment is controlled according to operational requirements, personal clearances, and data sensitivity. Policies provide for periodic evaluation of threats and vulnerabilities to ensure risks are known and appropriate safeguards are implemented. Policies also delineate data backup, contingency operations, incident handling, information storage, sharing, and transmission / transportation, malicious software protection, logging and audit, training, sanctions, disclosure, and personnel security requirements to ensure the confidentiality, integrity, and availability of the web servers and associated data. Each facility is responsible for conducting risk management processes and applying policies and procedures accordingly. Electronic and other personal data storage media, and associated computer equipment are stored in areas where fire and life safety codes are strictly enforced. Telecommunication equipment (computer terminal, modems and disks) are maintained in access controlled rooms during nonworking hours, Combinations on door locks are changed periodically and whenever an employee resigns, retires or is reassigned. Within each facility a list of personnel or categories of personnel having a demonstrable need for the records in the performance of their duties has been developed and is maintained. Procedures have been developed and implemented to review one-time requests for disclosure to personnel who may not be on the authorized user list. Proper charge-out procedures are followed for the removal of all records from the area in which they are maintained. Persons who have a need to know are entrusted with records from this system of records and are instructed to safeguard the confidentiality of these records. They are to make no further disclosure of the records except as authorized by the system manager and permitted by the Privacy Act, and to destroy all copies or to return such records when the need to know has expired. Procedural instructions include the statutory penalties for noncompliance. A profile of automated systems security is maintained. Security clearance procedures for screening individuals, both Government and contractor personnel, prior to their participation in the design, operation, use or maintenance of IHS automated information systems are implemented. The use of current passwords and log-on codes are required to protect sensitive automated data from unauthorized access. Such passwords and codes are changed periodically. An automated audit trail is maintained. Privacy Act requirements and specified Automated Information System security provisions are specifically included in contracts and agreements and the system manager or his/her designee oversee compliance with these contract requirements.

Richard G. Price
Jul 27, 2006
- 24 Sr Official of Privacy Signature:
- 25 Sr Official of Privacy Signoff Date:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

Summary of PIA Required Questions

Question

Response

- 1

System:
- IHS National Patient Information Reporting System (NPIRS)
- 2

Is this a new PIA?
- No
- 3

If this is an existing PIA, please provide a reason for revision:
- Initial PIA Migration to ProSight
- 4

Date of this Submission:
- Jul 27, 2006
- 5

OPDIV Name:
- IHS
- 6

Unique Project Identifier (UPI) Number:
- 009-17-01-00-01-1010-04 (009-17-01-20-01-1020-00-110-031; 917012001102000000000)
- 7

Privacy Act System of Records (SOR) Number:
- IHS PA System 09-17-0001
- 8

OMB Information Collection Approval Number:
- No
- 9

Other Identifying Number(s):
- No
- 10

System Name:
- National Patient Information and Reporting System (NPIRS)
- 11

System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- Stanley Griffith

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

- 12 Provide an overview of the system:
- 1.To provide a description of a individual's diagnosis, treatment and outcome, and to plan for immediate and future care of the individual.
2.To provide statistical data to IHS officials in order to evaluate health cre programs and to plan for future needs. 3.To serve as a means of communication among members of the health care team who contribute to the indivudal's care; e.g., to integrate information from field visits with records of treatment in IHS facilities and with non-IHS health care providers 4.To serve as the official docunmentation of an individual's health care 5.To contribute to continuing education of IHS staff ot improve the delivery of health care services. 6. For disease surveillance purposes. For example: (a) the Centers for Disease Control and Prevention may use these records to monitor various communicable diseases; (b) the National Institutes of Health may use these records to review the prevalence of particular diseases (e.g., malignant neoplasms, diabetes mellitus, arthritis, metabolism, and digestive diseases) for various ethnic groups of the United States; or (c) those public health authorities that are authorized by law may use these records to collect or receive such information for purposes of preventing or controlling disease, injury, or diability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death and the conduct of public health surveillance, investigations, and interventions. 7. To compile and provide aggregated program statistics. Upon request of other components of DHHS, IHS will provide statistical information, from which individual/personal identifiers ahve been removed, such as: (a) to the National Committeee on Vital and Health Statistics for its dissemination of aggregated health statistics on various ethnic groups; (b) to the Assistant Secretary for Planning and Evaluation, Health Policy to keep a record of the number of sterilizations provided by federal funding; (c) to the Centers for Medicare & Medicaid Services (CMS) to document IHS health care covered by the Medicare and Medicaid programs for third party reimbursement; or (d) to the Office of Clinical Standards and Quality, CMS to determine the prevalence of end-stage renal disease among the American Indian and Alaska Native (AI/AN) population and to coordinate individual care.
8. To process and collect third-party claims and facilitate fiscal intermediary functions and to process debt collection activities.
9. To improve the IHS national patient care database by means of obtaining and verifying an individual=s SSN with the Social Security Administration (SSA).
10. To provide information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs to facilitate organ, eye, or tissue donation and transplant.
11. To provide information to individuals about treatment alternatives or other types of health-related benefits and services.
12. To provide information to the Food and Drug Administration (FDA) in connection with an FDA-regulated product or activity.
13. To provide information to correctional institutions as necessary for health and safety purposes.
14. To provide information to governmental authorities (e.g., social services or protective services agencies) on victims of abuse, neglect, sexual assault or domestic violence.
15. To provide information to the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C ' 2901, et seq.
16. To provide relevant health care information to funeral directors or representatives of funeral homes to allow necessary arrangements prior to and in anticipation of an individual=s impending death.
- Existing
- 13 Indicate if the system is new or an existing one being modified:
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

- 15 Is the system subject to the Privacy Act?

Yes
- 16 If the system shares or discloses IIF please specify with whom and for what purpose(s):

Does not violate legal or policy limitations under which the record was provided, collected, or obtained. Law Enforcement Agencies: The IHS health care providers may disclose information from these records regarding the commission of crimes or the occurrence of communicable diseases, tumors, suspected child abuse, births, deaths, alcohol or drug abuse, etc., as required by Federal law or regulation or State or local law or regulation of the jurisdiction in which the facility is located. The IHS health care providers may disclose information from these records regarding suspected cases of child abuse. IHS Contractors: Records may be disclosed to an IHS contractor, including tribal contractors, for the purpose of computerized data entry or maintenance of records contained in this system. The contractor shall be required to maintain Privacy Act safeguards with respect to the receipt and processing of such records. Records may be disclosed to a health care provider under contract to IHS (including tribal contractors) to permit the contractor to obtain health and medical information about the subject individual in order to provide appropriate health services to that individual. The contractor shall be required to maintain Privacy Act safeguards with respect to the receipt and processing of such records. Student Volunteers: Records may be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for PHS who do not technically have the status of agency employees, if they need the records in the performance of their agency functions. The information is shared back to the customers in support of their regional programs. Information (i.e., statistical, patient demographic, facility or institutional, medical, research, education, disease management, eligibility, etc.) is shared with internal IHS agencies and external organizations with approvals from IHS/OPS and HIPAA.

1) Health and medical records containing examination, diagnostic and treatment data, proof of IHS eligibility, social data (such as name, address, date of birth, Social Security Number (SSN), tribe), laboratory test results, and dental, social service, domestic violence, sexual abuse and/or assault, mental health, and nursing information.

2) Follow-up registers of individuals with a specific health condition or a particular health status such as cancer, diabetes, communicable diseases, suspected and confirmed abuse and neglect, immunizations, suicidal behavior, or disabilities.

3) Logs of individuals provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.

4) Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.

5) Monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes.

6) Third-party reimbursement and billing records containing name, address, date of birth, dates of service, third party insurer claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to process and validate third-party reimbursement claims.

7) Contract Health Service (CHS) records containing name, address, date of birth, dates of care, Medicare or Medicaid claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to determine CHS eligibility and to process CHS claims.

8. Yes, contains IIF.

9. Mandatory submission of personal information.
- 17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

18 Describe the consent process:

Notification procedure

General Procedure: Requests must be made to the appropriate System Manager (IHS Area, Program Office Director or Service Unit Director/Chief Executive Officer). A subject individual who requests a copy of, or access to, his or her medical record shall, at the time the request is made, designate in writing a responsible representative who will be willing to review the record and inform the subject individual of its contents. Such a representative may be an IHS health professional. When a subject individual is seeking to obtain information about himself/ herself that may be retrieved by a different name or identifier than his/her current name or identifier, he/she shall be required to produce evidence to verify that he/she is the person whose record he/she seeks. No verification of identity shall be required where the record is one that is required to be disclosed under the Freedom of Information Act. Where applicable, fees for copying records will be charged in accordance with the schedule set forth in 45 CFR Part 5b.

Requests In Person: Identification papers with current photographs are preferred but not required. If a subject individual has no identification but is personally known to the designated agency employee, such employee shall make a written record verifying the subject individual's identity. If the subject individual has no identification papers, the responsible system manager or designated agency official shall require that the subject individual certify in writing that he/she is the individual whom he/she claims to be and that he/she understands that the knowing and willful request or acquisition of records concerning an individual under false pretenses is a criminal offense subject to a \$5,000 fine. If an individual is unable to sign his/her name when required, he/she shall make his/her mark and have the mark verified in writing by two additional persons.

Requests By Mail: Written requests must contain the name and address of the requester, his/her date of birth and at least one other piece of information that is also contained in the subject record, and his/her signature for comparison purposes. If the written request does not contain sufficient information, the System Manager shall inform the requester in writing that additional, specified information is required to process the request.

Requests by Telephone: Since positive identification of the caller cannot be established, telephone requests are not honored.

Parents, Legal Guardians and Personal Representatives: Parents of minor children and legal guardians or personal representatives of legally incompetent individuals shall verify their own identification in the manner described above, as well as their relationship to the individual whose record is sought. A copy of the child's birth certificate or court order establishing legal guardianship may be required if there is any doubt regarding the relationship of the individual to the patient.

Record access procedures

Same as Notification Procedures: Requesters may write, call or visit the last IHS facility where medical care was provided. Requesters should also provide a reasonable description of the record being sought. Requesters may also request an accounting of disclosures that have been made of their record, if any.

Contesting record procedures: Requesters may write, call or visit the appropriate IHS Area/Program Office Director or Service Unit Director/Chief Executive Officer at his/her address specified in

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

Appendix 1, and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Record source categories: Individual and/or family members, IHS health care personnel, contract health care providers, State and local health care provider organizations, Medicare and Medicaid

- | | | |
|----|--|-----|
| 19 | Does the system host a website? | Yes |
| 20 | Does the website have any information or pages directed at children under the age of thirteen? | No |
| 21 | Are there policies or guidelines in place with regard to the retention and destruction of IIF? | Yes |
| 22 | Are there technical controls present? | Yes |

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. **Note:** If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. **Note:** If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

- 23 Describe the IIF security controls:
- Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: File folders, ledgers, card files, microfiche, microfilm, computer tapes, disk packs, digital photo discs, and automated, computer-based or electronic files.

Retrievability: Indexed by name, record number, and SSN and cross-indexed.

Safeguards: Safeguards apply to records stored on-site and off-site.

1. Authorized Users: Access is limited to authorized IHS personnel, volunteers, IHS contractors, subcontractors, and other business associates in the performance of their duties. Examples of authorized personnel include: Medical records personnel, business office personnel, contract health staff, health care providers, authorized researchers, medical audit personnel, health care team members, and legal and administrative personnel on a need to know basis.

2. Physical Safeguards: Records are kept in locked metal filing cabinets or in a secured room or in other monitored areas accessible to authorized users at all times when not actually in use during working hours and at all times during non-working hours. Magnetic tapes, disks, other computer equipment (e.g., pc workstations) and other forms of personal data are stored in areas where fire and life safety codes are strictly enforced. Telecommunication equipment (e.g., computer terminal, servers, modems and disks) of the Resource and Patient Management System (RPMS) are maintained in locked rooms during non-working hours. Network (Internet or Intranet) access of authorized individual(s) to various automated and/or electronic programs or computers (e.g., desktop, laptop, handheld or other computer types) containing protected personal identifiers or personal health information (PHI) is reviewed periodically and controlled for authorizations, accessibility levels, expirations or denials, including passwords, encryptions or other devices to gain access. Combinations and/or electronic passcards on door locks are changed periodically and whenever an IHS employee resigns, retires or is reassigned.

3. Procedural Safeguards: Within each facility a list of personnel or categories of personnel having a demonstrable need for the records in the performance of their duties has been developed and is maintained. Procedures have been developed and implemented to review one-time requests for disclosure to personnel who may not be on the authorized user list. Proper charge-out procedures are followed for the removal of all records from the area in which they are maintained. Records may not be removed from the facility except in certain circumstances, such as compliance with a valid court order or shipment to the Federal Records Center(s). Persons who have a need to know are entrusted with records from this system of records and are instructed to safeguard the confidentiality of these records. These individuals are to make no further disclosure of the records except as authorized by the system manager and permitted by the Privacy Act and the HIPAA Privacy Rule as adopted, and to destroy all copies or to return such records when the need to know has expired. Procedural instructions include the statutory penalties for noncompliance.

The following automated information systems (AIS) security procedural safeguards are in place for automated health and medical records maintained in the RPMS. A profile of automated systems

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. **Note:** If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. **Note:** If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS National Patient Information Reporting System (NPIRS)

security is maintained. Security clearance procedures for screening individuals, both Government and contractor personnel, prior to their participation in the design, operation, use or maintenance of IHS AIS are implemented. The use of current passwords and log-on codes are required to protect sensitive automated data from unauthorized access. Such passwords and codes are changed periodically. An automated or electronic audit trail is maintained and reviewed periodically. Only authorized IHS Division of Information Resources staff may
Richard G. Price
Jul 31, 2006

24 Sr Official of Privacy Signature:
25 Sr Official of Privacy Signoff Date:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

Summary of PIA Required Questions

Question

Response

- 1 System:
- IHS Resource Patient Management System (RPMS)
- 2 Is this a new PIA?
- No
- 3 If this is an existing PIA, please provide a reason for revision:
- Initial PIA Migration to ProSight
- 4 Date of this Submission:
- Jul 27, 2006
- 5 OPDIV Name:
- IHS
- 6 Unique Project Identifier (UPI) Number:
- 009-17-01-06-01-1010--110-031
- 7 Privacy Act System of Records (SOR) Number:
- 09-17-0001
- 8 OMB Information Collection Approval Number:
- No
- 9 Other Identifying Number(s):
- No
- 10 System Name:
- Resource and Patient Management System (RPMS)
- 11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- Howard Hays

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

- 12 Provide an overview of the system:
1. To provide a description of an individual's diagnosis, treatment and outcome, and to plan for immediate and future care of the individual.

2. To provide statistical data to IHS officials in order to evaluate health care programs and to plan for future needs.

3. To serve as a means of communication among members of the health care team who contribute to the individual's care; e.g., to integrate information from field visits with records of treatment in IHS facilities and with non-IHS health care providers.

4. To serve as the official documentation of an individual's health care.

5. To contribute to continuing education of IHS staff to improve the delivery of health care services.

6. For disease surveillance purposes. For example:

(a) the Centers for Disease Control and Prevention may use these records to monitor various communicable diseases;

(b) the National Institutes of Health may use these records to review the prevalence of particular diseases (e.g., malignant neoplasms, diabetes mellitus, arthritis, metabolism, and digestive diseases) for various ethnic groups of the United States; or

(c) those public health authorities that are authorized by law may use these records to collect or receive such information for purposes of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death and the conduct of public health surveillance, investigations, and interventions.

7. To compile and provide aggregated program statistics. Upon request of other components of DHHS, IHS will provide statistical information, from which individual/personal identifiers have been removed, such as:

(a) to the National Committee on Vital and Health Statistics for its dissemination of aggregated health statistics on various ethnic groups;

(b) to the Assistant Secretary for Planning and Evaluation, Health Policy to keep a record of the number of sterilizations provided by federal funding;

(c) to the Centers for Medicare & Medicaid Services (CMS) to document IHS health care covered by the Medicare and Medicaid programs for third-party reimbursement; or

(d) to the Office of Clinical Standards and Quality, CMS to determine the prevalence of end-stage renal disease among the American Indian and Alaska Native (AI/AN) population and to coordinate individual care.

8. To process and collect third-party claims and facilitate fiscal intermediary functions and to process debt collection activities.

9. To improve the IHS national patient care database by means of obtaining and verifying an individual's SSN with the Social Security Administration (SSA).

10. To provide information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs to facilitate organ, eye, or tissue donation and transplant.

11. To provide information to individuals about treatment alternatives or other types of health-related benefits and services.

12. To provide information to the Food and Drug Administration (FDA) in connection with an FDA-regulated product or activity.

13. To provide information to correctional institutions as necessary for health and safety purposes.

14. To provide information to governmental authorities (e.g., social services or protective services agencies) on victims of abuse, neglect, sexual assault or domestic violence.

15. To provide information to the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C ' 2901, et seq.

16. To provide relevant health care information to funeral directors or representatives of funeral homes to allow necessary arrangements

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. **Note:** If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. **Note:** If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

- 13

Indicate if the system is new or an existing one being modified:
- prior to and in anticipation of an individual's impending death.

Existing
- 14

Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- Yes
- 15

Is the system subject to the Privacy Act?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

- 16 If the system shares or discloses IIF please specify with whom and for what purpose(s):
1. Records may be disclosed to Federal and non-Federal (public or private) health care providers that provide health care services to IHS individuals for purposes of planning for or providing such services, or reporting results of medical examination and treatment.

2. Records may be disclosed to Federal, state, local or other authorized organizations that provide third-party reimbursement or fiscal intermediary functions for the purposes of billing or collecting third-party reimbursements. Relevant records may be disclosed to debt collection agencies under a business associate agreement arrangement directly or through a third party.

3. Records may be disclosed to state agencies or other entities acting pursuant to a contract with CMS, for fraud and abuse control efforts, to the extent required by law or under an agreement between IHS and respective state Medicaid agency or other entities.

4. Records may be disclosed to school health care programs that serve AI/AN for the purpose of student health maintenance.

5. Records may be disclosed to the Bureau of Indian Affairs (BIA) or its contractors under an agreement between IHS and the BIA relating to disabled AI/AN children for the purposes of carrying out its functions under the Individuals with Disabilities Education Act (IDEAS), 20 U.S.C. 1400, et seq.

6. Records may be disclosed to organizations deemed qualified by the Secretary of DHHS and under a business associate agreement to carry out quality assessment/improvement, medical audits, utilization review or to provide accreditation or certification of health care facilities or programs.

7. Records may be disclosed under a business associate agreement to individuals or authorized organizations sponsored by IHS, such as the National Indian Women=s Resource Center, to conduct analytical and evaluation studies.

8. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. An authorization, Form IHS 810, is required for the disclosure of sensitive protected health information (PHI) (e.g., alcohol/drug abuse patient information, human immunodeficiency virus (HIV)/AIDS, STD, or mental health) that is maintained in the medical record.

9. Records may be disclosed for research purposes to the extent permitted by:

(a) determining that the use(s) or disclosure(s) are met under 45 CFR ' 164.512(i), or

(b) determining that the use(s) or disclosure(s) are met under 45 CFR ' 164.514(a) through (c) for de-identified PHI, and 5 U.S.C. 552a (b)(5), or

(c) determining that the requirements of 45 CFR ' 164.514 (e) for limited data sets, and 5 U.S.C. 552a (b)(5) are met.

10. Information from records, such as information concerning the commission of crimes, suspected cases of abuse (including child, elder and sexual abuse), neglect, sexual assault or domestic violence, births, deaths, alcohol or drug abuse, immunizations, cancer, or the occurrence of communicable diseases, may be

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

disclosed to public health authorities or other appropriate government authorities, as authorized by Federal, state, Tribal or local law or regulation of the jurisdiction in which the facility is located.
Note: In Federally conducted or assisted alcohol or drug abuse programs, under 42 CFR Part 2, disclosure of patient information for purposes of criminal investigations must be authorized by court order issued under 42 CFR Part 2.65, except that reports of suspected child abuse may be made to the appropriate state or local authorities under state law.

11. Information may be disclosed from these records regarding suspected cases of child abuse to:

(a) Federal, state or Tribal agencies that need to know the information in the performance of their duties, and

(b) members of community child protection teams for the purposes of investigating reports of s

- 1) Health and medical records containing examination, diagnostic and treatment data, proof of IHS eligibility, social data (such as name, address, date of birth, Social Security Number (SSN), tribe), laboratory test results, and dental, social service, domestic violence, sexual abuse and/or assault, mental health, and nursing information.
- 2) Follow-up registers of individuals with a specific health condition or a particular health status such as cancer, diabetes, communicable diseases, suspected and confirmed abuse and neglect, immunizations, suicidal behavior, or disabilities.
- 3) Logs of individuals provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.
- 4) Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.
- 5) Monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes.
- 6) Third-party reimbursement and billing records containing name, address, date of birth, dates of service, third party insurer claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to process and validate third-party reimbursement claims.
- 7. Contract Health Service (CHS) records containing name, address, date of birth, dates of care, Medicare or Medicaid claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to determine CHS eligibility and to process CHS claims.

- 8. Yes, contains IIF.
- 9. Mandatory submission of personal information.

17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

- 18 Describe the consent process:

A. New patients must be registered in the IHS facility data base prior to being provided health care services; however, emergency services should not be delayed. Information on patients who present a critical emergency that requires immediate medical attention must be obtained from the patient's relative or other accompanying individual. Each patient's IHS registration information is updated on each subsequent visit to the facility by personal interview conducted by a designated IHS facility staff member. The patient registration process at each IHS facility is accomplished by using the IHS Patient Registration System (PRS) software and the technical guidelines in Chapter 2, "Patient Registration" of the IHS Business Office Manual.

B. The service unit has the responsibility to encourage all patients who are registered to present any documentation they might have relative to their eligibility-for IHS health care services and alternate resources. These documents will greatly assist in maintaining accurate patient information in the PRS data base.

C. Patients are requested to bring their Social Security card, private insurance identification, and other information (such as proof of tribal affiliation and blood quantum) to initial or subsequent patient registration interviews. Registration staff explains to the patients that such information will expedite the patient registration and eligibility determination process. Patients' mailing addresses and personal information files are kept updated so that all health care benefits can be identified and expedited, and be utilized by the health care provider.

D. All IHS staff are sensitive to IHS patients cultural values and concerns for privacy. Patient registration is a vital part of each IHS facility's public relations program and patient registration staff receive continuous management support for maintaining skills in communicating with the patients and assuring the patients' comfort during the interview process.

E. Confidentiality of patient information collected is maintained at all times in accordance with the Privacy Act of 1974. The registration staff periodically reviews the Privacy Act. The registration staff informs the patient of the requirements of the Privacy Act, and the date is entered into the PRS.

F. The patient must authorize release of Medicare/Railroad Insurance information, and the date the authorization was obtained is entered into the PRS by registration staff.
- 19 Does the system host a website?

Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

IHS: IHS Resource Patient Management System (RPMS)

23 Describe the IIF security controls:

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
Storage: File folders, ledgers, card files, microfiche, microfilm, computer tapes, disk packs, digital photo discs, and automated, computer-based or electronic files.
Retrievability: Indexed by name, record number, and SSN and cross-indexed.
Safeguards: Safeguards apply to records stored on-site and off-site.
1. Authorized Users: Access is limited to authorized IHS personnel, volunteers, IHS contractors, subcontractors, and other business associates in the performance of their duties. Examples of authorized personnel include: Medical records personnel, business office personnel, contract health staff, health care providers, authorized researchers, medical audit personnel, health care team members, and legal and administrative personnel on a need to know basis.
2. Physical Safeguards: Records are kept in locked metal filing cabinets or in a secured room or in other monitored areas accessible to authorized users at all times when not actually in use during working hours and at all times during non-working hours. Magnetic tapes, disks, other computer equipment (e.g., pc workstations) and other forms of personal data are stored in areas where fire and life safety codes are strictly enforced. Telecommunication equipment (e.g., computer terminal, servers, modems and disks) of the Resource and Patient Management System (RPMS) are maintained in locked rooms during non-working hours. Network (Internet or Intranet) access of authorized individual(s) to various automated and/or electronic programs or computers (e.g., desktop, laptop, handheld or other computer types) containing protected personal identifiers or personal health information (PHI) is reviewed periodically and controlled for authorizations, accessibility levels, expirations or denials, including passwords, encryptions or other devices to gain access. Combinations and/or electronic passcards on door locks are changed periodically and whenever an IHS employee resigns, retires or is reassigned.
3. Procedural Safeguards: Within each facility a list of personnel or categories of personnel having a demonstrable need for the records in the performance of their duties has been developed and is maintained. Procedures have been developed and implemented to review one-time requests for disclosure to personnel who may not be on the authorized user list. Proper charge-out procedures are followed for the removal of all records from the area in which they are maintained. Records may not be removed from the facility except in certain circumstances, such as compliance with a valid court order or shipment to the Federal Records Center(s). Persons who have a need to know are entrusted with records from this system of records and are instructed to safeguard the confidentiality of these records. These individuals are to make no further disclosure of the records except as authorized by the system manager and permitted by the Privacy Act and the HIPAA Privacy Rule as adopted, and to destroy all copies or to return such records when the need to know has expired. Procedural instructions include the statutory penalties for noncompliance.
The following automated information systems (AIS) security procedural safeguards are in place for automated health and medical records maintained in the RPMS. A profile of automated systems security is maintained. Security clearance procedures for screening individuals, both Government and contractor personnel, prior to their participation in the design, operation, use or maintenance of IHS AIS are implemented. The use of current passwords and log-on codes are required to protect sensitive automated data from unauthorized access. Such passwords and codes are changed periodically. An automated or electronic audit trail is maintained and reviewed periodically. Only authorized IHS Division of Information Resources staff may modify automated fil
Richard G. Price
Jul 31, 2006

24 Sr Official of Privacy Signature:
25 Sr Official of Privacy Signoff Date:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.